

UNITED STATES DISTRICT COURT

for the
District of South CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)User Account: greekword9@gmail.com
located on the servers of Dropbox, Inc., 1800 Owens
Street, Suite 200, San Francisco, California 94158

Case No. 6:20-cr-00341

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.

located in the _____ District of _____ South Carolina _____, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2252
18 U.S.C. § 2252A

Offense Description
Receipt or Distribution of Visual Depictions of Sexually Explicit Conduct
Receipt and Distribution of Child Pornography

The application is based on these facts:
See attached affidavit.

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Appeared & Sworn by telephone
Daniel Cutts

Applicant's signature

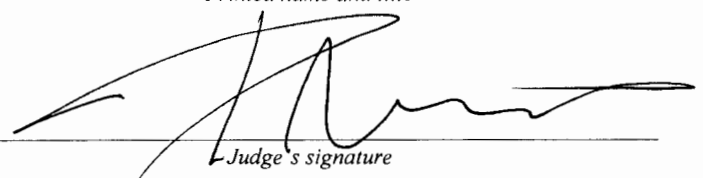
Daniel Cutts, SA

Printed name and title

Sworn to before me and signed ~~in my presence.~~ ^{by telephone}

Date: 05/15/2020

City and state: Greenville, SC



Judge's signature

Kevin F. McDonald, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA

IN THE MATTER OF THE SEARCH OF:

User Account: greeksword9@gmail.com

located on the servers of Dropbox, Inc., 1800
Owens Street, Suite 200, San Francisco,
California 94158

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Daniel Cutts, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search of Dropbox, Inc., an online storage service, physically located at 1800 Owens Street, Suite 200, San Francisco, California 94158, more particularly described in Attachment A, specifically to search for and seize instrumentalities, fruits and evidence of violations of 18 U.S.C. §§ 2252 and 2252A (possession, receipt, and transportation of child pornography and other related materials). The items that are the subject of the search and seizure applied for in this affidavit are more specifically described in Attachment B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), which require Dropbox, Inc. to disclose to the Government, records and other information in its possession, including the contents of communications, pertaining to “greeksword9@gmail.com.” As set forth herein, probable cause exists to believe that evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of 18 U.S.C. § 2252A, may be found in Dropbox, Inc.’s records.

2. I have been employed as a Special Agent since July 2002, for the Department of Homeland Security, Homeland Security Investigations (DHS-HSI). Prior to my employment with DHS-HSI, I was employed as an Inspector with the United States Customs Service. I held this position from 1997 until 2001 when I accepted a position with the United States Customs Service, Office of Investigations. As an Inspector, I was involved with the enforcement of federal law governing the importation and exportation of goods into and out of the United States. As a Special Agent with DHS-HSI, my responsibilities include identifying individuals and entities involved in violations of federal law and investigating their activities for presentation to the United States Attorney's Office for criminal prosecution. Among the federal laws enforced by DHS-HSI are Title 18, United States Code, Section 2252(a) and 2252A, the illegal production, distribution, receipt and possession of child pornography. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in Title 18, United States Code, Section 2252) in all forms of media, including computer media. I have participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses. In June 2008, I graduated from the Treasury Computer Forensics Training Program (TCFTP) and the Preliminary Basic Computer Evidence Recovery Training Program (PBCERT) held at the Federal Law Enforcement Training Center in Glynco, Georgia. This training has afforded me the skills and techniques necessary to recover and analyze evidence stored on a computer system and I am now a certified Computer Forensics Agent (CFA) for HSI Greenville, South Carolina. I have successfully completed several computer examinations and recovered evidence which has led to several state and federal prosecutions. I have a Bachelors Degree in Criminal Justice. As an HSI Special Agent, I am authorized under

18 U.S.C. § 545 to investigate violations of certain criminal statutes, including 18 U.S.C. § 1442 (prohibiting the importation of any obscene or lascivious book, pamphlet, or picture); 18 U.S.C. § 1466 (prohibiting the engaging in the business of selling or transferring obscene matter); and 18 U.S.C. § 2251 et seq. (prohibiting the sexual exploitation of children). This includes violations of 18 U.S.C. §§ 2252, 2252A, which make it a federal offense to knowingly possess, access, transport, receive or distribute a visual depiction involving the use of a minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256, if such visual depiction has been mailed, shipped, or transported using any means of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, or the visual depiction was produced using any materials that have been so mailed, shipped, or transported.

3. The facts in this affidavit come from my personal observations; my training; my experience; information obtained from reviewing documents and records; and other law enforcement officers and witnesses. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of 18 U.S.C. § 2252A are currently with Dropbox, Inc.'s custodian of records located at 1800 Owens Street, Suite 200, San Francisco, California, 94107. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. § 2252A, related to material involving the sexual exploitation of minor. 18 U.S.C. § 2252A states in pertinent part:

(a) [a]ny person who

(2) knowingly receives or distributes

(A) any child pornography that has been mailed or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means including by computer[.]

(5)

(B) knowingly possesses, or knowingly accesses with intent to view any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer[.]

18 U.S.C. § 2252A(a)(2)-(5).

JURISDICTION & VENUE

5. The legal authority for this search and seizure warrant application is derived from 18 U.S.C §§ 2701-11, entitled, “stored wire and electronic communications and transactional records access.” *See* U.S.C. 18 § 2701. Nationwide service of process of search and seizure warrants for the contents of electronic communications is permitted. *See* 18 U.S.C. §

2703(c)(A). A government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction. *See* 18 U.S.C. § 2703(a).

6. This Court is “a district court of the United States...that—has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711; *see* 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for South Carolina since “greekword9@gmail.com,” which was used to create a Dropbox account containing child pornography and was accessed by a subject by the name of Demetrius JOHN within the District of South Carolina. *See* 18 U.S.C. §§ 3237(a), §3231, and 3232.

DEFINITIONS

7. The term “minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

8. The term “child pornography” means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where “the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.” 18 U.S.C. § 2256(8)(A)-(C).

9. The term “sexually explicit conduct” means any actual or simulated “sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.” 18 U.S.C. § 2256(2)(A)(i)-(v).

10. For the purposes of this affidavit, unless otherwise specifically indicated, the term “computer,” as defined in 18 U.S.C. § 1030(e)(1), refers to the box that houses the central processing unit (“CPU”), along with any internal storage devices (such as internal hard drives) and internal communication devices (such as internal modems capable of sending or receiving email or fax cards) along with any other hardware stored or housed internally. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term computer system is used. Information refers to all the information on a computer system including both software applications and data.

11. “Internet Protocol Address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (“ISP”) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

12. The term “domain name” refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards,

from right to left, further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

13. The term “log files” includes records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

14. “Contents” as used with respect to any wire, oral, or electronic communication, includes any information, concerning the substance, purport, or meaning of that communication. *See* 18 U.S.C. § 2510(8).

15. “Electronic Communications System” means any wire, radio, electromagnetic, photo optical, or photo electronic facility used for the transmission of wire or electronic communications, and any computer facilities, or related electronic equipment for the electronic storage of such communications. *See* 18 U.S.C. § 2510(14).

16. “Electronic Communication Service” means any service which provides to users thereof the ability to send or to receive wire or electronic communications. *See* 18 U.S.C. § 2510(15).

17. The term “remote computing service” means any service which provides to users thereof computer storage or processing services by means of an “electronic communications system.” *See* 18 U.S.C. § 2711(2).

18. The term “electronic storage” means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, and any storage of such communication by an electronic communication service for purposes of backup protection of such communication. *See* 18 U.S.C. § 2510(17). Typically, email that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that email to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage constitutes “electronic storage”.

19. The term “computer hardware” as used in this affidavit refers to all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data processing devices (such as central processing units, memory typewriters, and self-contained laptops or notebook computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, “RAM” or “ROM” units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone generating devices); as well as any

devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

20. The term “computer software” as used in this affidavit refers to digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

21. The term “computer-related documentation” refers to written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

STATEMENT OF PROBABLE CAUSE

22. On or about December 2, 2019, Homeland Security Investigations (HSI) Special Agents in Newark, New Jersey, acting in an online undercover (UC) capacity commenced communications over ProtonMail with a user using the email address flinjake23@gmail.com. During the course of their communications, the user using email address flinjake23@gmail.com, discussed wanting to obtain and trade child pornography. On or about December 4, 2019, the user using email address flinjake23@gmail.com requested for the UC to begin communication over the platform Wickr. Before transitioning to Wickr from ProtonMail, the UC instructed the subject to send a unique code to ensure that the communications were coming from the same person. On Wickr, the user using email address flinjake23@gmail.com, used the Wickr screenname “greek sword” and sent the UC the same unique code as requested by the UC. User “greek sword” also sent four (4) videos depicting child pornography. The subject told the UC

that he/she was especially interested in “little girls” being ejaculated on by adult men which is consistent with the videos that were sent.

23. HSI Newark provided the four (4) videos to your affiant for review. The videos are more particularly described below.

- a. File “VID-20191023-WA0244.mp4”. This video is approximately three minutes and fifty-six seconds and it depicts a pre-pubescent female performing oral sex on what appears to be an adult male.
- b. File “VID-20170930-WA0013.mp4”. This video is approximately thirty eight seconds and it depicts a pre-pubescent female in a car, on the lap of what appears to be an adult female and rubbing what appears to be an adult male’s penis.
- c. File “VID_20191115_063334_903.mp4”. This video is approximately nineteen seconds and it depicts a minor female performing oral sex on what appears to be an adult male.
- d. File “VID_20191024_170043_155.mp4”. This video is approximately fifty four seconds and it depicts what appears to be an adult male masturbating on a nude, pre-pubescent female who is sitting on a toilet.

24. Based on this investigation, on March 11, 2020, HSI Greenville, along with the Anderson County Sheriff’s Office (ACSO) and the South Carolina Attorney General’s Office (SCAGO) executed a federal search warrant on the residence of Demetrius JOHN, located at 1100 E. Market Street, Apartment 14B, Anderson, South Carolina 29624. JOHN was present during the search warrant and he agreed to speak with law enforcement regarding this investigation. During the interview, JOHN admitted to possessing and distributing child

exploitive material using various social media outlets as well as using online storage services of Dropbox to store child exploitive material. JOHN stated that he uses his Gmail email address, greekword9@gmail.com, to sign into Dropbox. An onsite extraction of a cellular telephone belonging to JOHN resulted in the discovery of several video files containing child exploitive material.

CHARACTERISTIC OF INDIVIDUALS WITH SEXUAL INTEREST IN CHILDREN

25. My training, experience, and discussions with other investigators who have investigated child pornography and the exploitation of children for many years, have taught me that persons who have a sexual interest in children and/or who produce, trade, distribute, or possess depictions of minors engaged in sexually explicit conduct generally exhibit the following characteristics:

- a. These individuals view children as sexual objects and receive gratification from sexually explicit images of minors;
- b. These individuals collect sexually explicit images of minors that they use for their own sexual gratification and fantasy. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel deviant sexual fantasies involving children;
- c. My training, experience, and discussions with other investigators have further taught me that these people tend to keep their images for periods exceeding several years. They keep these sexually explicit images of minors for such long periods of time because the images are treated as prized possessions. They store

such images in different formats including photos, printouts, magazines, videotapes, and digital media formats such as hard drives, diskettes, and CDs;

- d. These individuals use sexually explicit images of minors as a means of reliving fantasies or actual sexual encounters. They also use the images as keepsakes and as a means of gaining acceptance, status, trust, and psychological support by exchanging, trading, or selling the images to other people with similar interests either in person or via the Internet. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, email, email groups, bulletin boards, Internet Relay Chat, newsgroups, instant messaging, and other similar vehicles;
- e. These individuals go to great lengths to conceal and protect from discovery their collection of sexually explicit images of minors. They may have passwords used to access programs or control encryption written down either in the vicinity of their computer or on their person (for instance, in their wallet or an address book); and
- f. These individuals maintain images of minors with whom they have had sexual contact. If a picture of a minor is taken by such a person depicting the minor in the nude, there is a high probability that the minor was used to produce sexually explicit images to be traded with people with similar interests.

26. In addition, your affiant's experience and training has shown that such material is normally and generally kept in the individual's office, residence, automobile, email accounts, virtual storage platforms like the iCloud or Dropbox, or other secure location to ensure convenient and ready access.

27. In my training and experience conducting child exploitation investigations, I am aware that persons who receive, possess and distribute images of child pornography sometimes utilize email accounts and online storage accounts to correspond with other persons sharing similar interests; and that those persons also sometimes utilize those accounts to receive, transmit and store images of child pornography.

28. The visual images obtained, traded or sold are prized by child pornography collectors and have value to the collector. The visual images are intrinsically valuable for trading or selling and therefore are rarely destroyed or deleted by the collector.

BACKGROUND ON CHILD PORNOGRAPHY AND ON THE USE OF TECHNOLOGY

29. Pursuant to your affiant's training and experience, as well as the training and experience of other law enforcement personnel, your affiant has learned that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contacts with other individuals who have it available. The use of the internet to traffic in, trade or collect child pornography has become one of the preferred methods of obtaining child pornography. An individual familiar with the internet can use the internet, usually in the privacy of the individual's home, to interact with another individual or a business offering such materials. The use of the internet offers individuals interested in obtaining child pornography a sense of privacy and secrecy not available elsewhere. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric or other special characters) usually operates as a "digital key" to "unlock" particular data security devices. Data security hardware may include encryption devices, chips,

and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

30. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls. Any reimbursement would follow these same paths. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

31. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods. Child pornography obtained via the internet can be saved to a variety of electronic media, including hard disk drives, flash memory devices, CDs, DVDs, and others. The ability to easily produce child pornography, inexpensively reproduce it, and anonymously market it (through electronic communications) changed the method of distribution of child pornography. Child pornography can now be electronically mailed to anyone with access to a

computer and access to the Internet. With the proliferation of commercial services and chat services, the computer has become one, if not the preferred, method of distribution of pornographic materials.

DROPBOX

32. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, found at <https://www.dropbox.com/privacy>, Dropbox collects and stores "your files, documents, photos, comments, messages and so on". Dropbox also stores related information, including profile information, file metadata, and usage activity. Moreover, Dropbox collects and stores usage and device information, including IP addresses, the type of browser and device used to connect to Dropbox, other web pages visited prior to visiting Dropbox's website, and other device identifiers.

33. Your affiant knows from training and experience that Dropbox users can increase their amount of storage space by referring friends connected with social media, referred to as collaborators. Dropbox's privacy policy states that it maintains information about the user's collaborators.

34. Your affiant knows from training and experience that Dropbox allows a user to synchronize their browser bookmarks. Bookmarks are often called favorites and serve as a shortcut to a specific webpage. A person soliciting, trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the sexual abuse of children may bookmark the webpages of their favorite sites used to view or download or disseminate more files involving the exploitation of minors.

35. Your affiant understands from training and experience that persons soliciting,

trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the sexual abuse of children and creation of files depicting exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of these images as well as provide evidence of a persons interest in child exploitive material or child exploitation. This communication could occur via email or text via computers or mobile devices. Your affiant is aware that email and text message information may be stored via a Dropbox account and a user can utilize Dropbox as a default documents folder. Files can be sent as attachments through a custom email address and those files would reside in the user's Attachment folder in Dropbox. Dropbox also allows a user to sync instant messaging transcripts. Communication between the user and other individuals interested in the soliciting, trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the sexual abuse of children and creation of files depicting exploitation of children may be saved within a Dropbox account.

36. Your affiant understands from training and experience that metadata is associated with files and assists in describing files. Metadata could consist of the name of the person who created a file, the date the file was created, the file size or the date a file was modified. Metadata is used for documents as well as images, videos and webpages. The author of the file can create the metadata so that he can describe and easily locate the file later. Metadata stored by Dropbox as it relates to a user's account will assist in showing when a file was last modified or when an image file was created. Dropbox keeps a history of file changes so that the user can access a previous version of a file prior to changes.

SEARCH METHODOLOGY TO BE EMPLOYED

37. Your affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

38. The government will retain a complete copy of the information received from Dropbox, Inc. for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligation by destroying data or returning it to a third party.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is required for the service or execution of this warrant.

40. Additionally, to ensure compliance with 18 U.S.C. § 2252(A), Dropbox does not mail, transport or deliver by computer child pornography to any person other than as permitted as part of making a report to the National Center for Missing and Exploited Children pursuant to 18 U.S.C. § 2258. Accordingly, absent permission by the Court, Dropbox will not transmit information responsive to this warrant should it contain, as is anticipated, child pornography. The Court has the authority to order Dropbox to disclose responsive data to the Court's search warrant by sending it to the Government using the U.S. Postal Service or anything courier service, notwithstanding 18 U.S.C. § 2252(A), or similar statute or code.

Dropbox routinely complies with such orders, which do not place any unreasonable burden on Dropbox. Accordingly, Attachment B allows for Dropbox to comply with the warrant by sending results to your affiant by U.S. Mail or other courier.

CONCLUSION

41. Based on the facts of the investigation detailed above in this Affidavit, coupled with my training and experience as an HSI Special Agent, your affiant asserts there is probable cause to believe that the information associated with Dropbox account greekword9@gmail.com stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., contains evidence of violations of 18 U.S.C. § 2252A. The information associated with Dropbox account greekword9@gmail.com will identify its owner, and the contraband contained therein. Therefore, your Affiant respectfully requests that the Court issue a warrant for the search of the account described in Attachment A and for the search and seizure of the items more fully described in Attachment B. Because the warrant will be served on Dropbox, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

42. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the Dropbox account “greekword9@gmail.com” that is stored at the premises owned, maintained, controlled, or operated by Dropbox, Inc., a company headquartered at 1800 Owens Street, Suite 200, California 94043, and authorizing the search and seizure of the items described in Attachment B.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

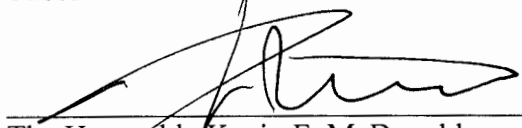
Respectfully submitted,

Appeared & Sworn by telephone

Daniel Cutts

Daniel Cutts
Special Agent
United States Department of Homeland Security
Homeland Security Investigations

by telephone
Subscribed and sworn to ~~before me~~ on this 15 day of May, 2020.


The Honorable Kevin F. McDonald
United States Magistrate Judge
District of South Carolina

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The Dropbox, Inc. account greeksword9@gmail.com that is stored at premises owned, maintained, controlled or operated by:

Dropbox, Inc.

1800 Owens Street, Suite 200

San Francisco, California 94158

ATTACHMENT B**PARTICULAR ITEMS TO BE SEIZED
INFORMATION TO BE DISCLOSED BY DROPBOX, INC.**

1. To the extent that the information described in Attachment A is within the possession, custody or control of Dropbox, Inc., hereinafter referred to as The Provider, regardless of whether such information is stored, held, or maintained inside or outside of the United States, and including any records, files, logs or information that has been deleted but still available to The Provider or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), The Provider is required to disclose the following information to the Government for each account, or identifier, listed in Attachment A.

2. All records or other information regarding the identification of the account and the types of service utilized, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files and means and source of payment (including any credit or bank account numbers), if applicable; records of session times and durations, types of service utilized, address books, contact and buddy lists, calendar data, pictures and files, all records pertaining to communications between The Provider and any person regarding this account, including contacts with support services and records of actions taken;

3. All multimedia files, in any format, pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession,

receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. All information related to other accounts associated with this account as a result of referrals or otherwise being a collaborator or contact.

5. All information related to bookmarks or newsgroup information related to this user account.

6. All information related to communications and/or correspondence with other subjects that may be stored in the user account.

7. All information related to information found in the Attachment folder within the user account as well as any information related to instant messaging that may be stored in the user account.

8. All Metadata information related to the user account.